Introducing the Sensor

This chapter introduces the sensor and provides information you should know before you install the sensor. In this guide, the term sensor refers to all models unless noted otherwise. For a complete list of supported sensors and their model numbers, see Supported Sensors, page 1-11.

This chapter contains the following sections:

- How the Sensor Functions, page 1-1
- Supported Sensors, page 1-11
- Appliances, page 1-13
- Modules, page 1-15
- Time Sources and the Sensor, page 1-19
- Installation Preparation, page 1-21
- Site and Safety Guidelines, page 1-22
- Cable Pinouts, page 1-25

How the Sensor Functions

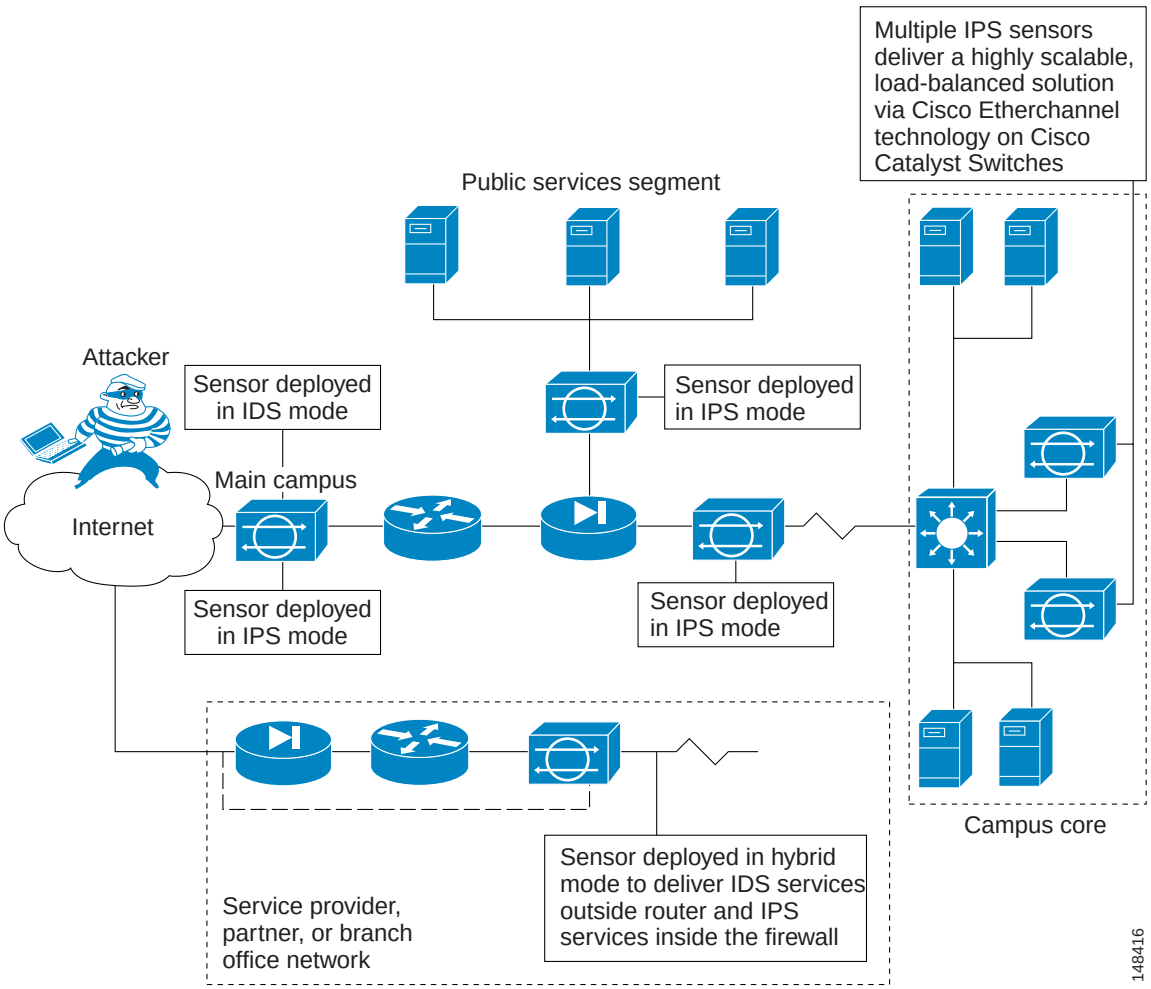
This section describes how the sensor functions and contains the following topics:

- Capturing Network Traffic, page 1-1
- Sensor Interfaces, page 1-3
- Interface Modes, page 1-9
- Your Network Topology, page 1-11

Capturing Network Traffic

The sensor can operate in either promiscuous or inline mode. Figure 1-1 on page 1-2 shows how you can deploy a combination of sensors operating in both inline (IPS) and promiscuous (IDS) modes to protect your network.

Figure 1-1 Comprehensive Deployment Solutions


Multiple IPS sensors deliver a highly scalable, load-balanced solution via Cisco Etherchannel technology on Cisco Catalyst Switches
Public services segment
Attacker
Sensor deployed in IDS mode
Sensor deployed in IPS mode
Main campus
Internet
Sensor deployed in IPS mode
Sensor deployed in IPS mode
Campus core
Sensor deployed in hybrid mode to deliver IDS services outside router and IPS services inside the firewall
Service provider, partner, or branch office network
148416

Note IDS-4210 and NM-CIDS do not operate in inline mode.

The command and control interface is always Ethernet. This interface has an assigned IP address, which allows it to communicate with the manager workstation or network devices (Cisco switches, routers, and firewalls). Because this interface is visible on the network, you should use encryption to maintain data privacy. SSH is used to protect the CLI and TLS/SSL is used to protect the manager workstation. SSH and TLS/SSL are enabled by default on the manager workstations.

When responding to attacks, the sensor can do the following:

- Insert TCP resets via the sensing interface.

  Note You should select the TCP reset action only on signatures associated with a TCP-based service. If selected as an action on non-TCP-based services, no action is taken. Additionally, TCP resets are not guaranteed to tear down an offending session because of limitations in the TCP protocol. On the IDS-4250-XL, TCP resets are sent through the TCP reset interface.

- Make ACL changes on switches, routers, and firewalls that the sensor manages.

Note ACLs may block only future traffic, not current traffic.

- Generate IP session logs, session replay, and trigger packets display.

  IP session logs are used to gather information about unauthorized use. IP log files are written when events occur that you have configured the appliance to look for.
- Implement multiple packet drop actions to stop worms and viruses.

Sensor Interfaces

The sensor interfaces are named according to the maximum speed and physical location of the interface. The physical location consists of a port number and a slot number. All interfaces that are built-in on the sensor motherboard are in slot 0, and the PCI expansion slots are numbered beginning with slot 1 for the bottom slot with the slot numbers increasing from bottom to top. Interfaces with a given slot are numbered beginning with port 0 for the right port with the port numbers increasing from right to left. For example, GigabitEthernet2/1 supports a maximum speed of 1 Gigabit and is the second-from-the-right interface in the second-from-the bottom PCI expansion slot. IPS-4240, IPS-4255, and IPS-4260 are exceptions to this rule. The command and control interface on these sensors is called Management0/0 rather than GigabitEthernet0/0.

There are three interface roles:

- Command and control
- Sensing
- Alternate TCP reset.

There are restrictions on which roles you can assign to specific interfaces and some interfaces have multiple roles. You can configure any sensing interface to any other sensing interface as its TCP reset interface. The TCP reset interface can also serve as an IDS (promiscuous) sensing interface at the same time. The following restrictions apply:

- Because NM-CIDS and AIP-SSM only have one sensing interface, you cannot configure a TCP reset interface.
- Because of hardware limitations on the Catalyst switch, both of the IDSM-2 sensing interfaces are permanently configured to use System0/1 as the TCP reset interface.
- The TCP reset interface that is assigned to a sensing interface has no effect in inline interface or inline VLAN pair mode, because TCP resets are always sent on the sensing interfaces in those modes.

This section contains the following topics:

- Command and Control Interface, page 1-4
- Sensing Interfaces, page 1-4
- Interface Support, page 1-5
- TCP Reset Interfaces, page 1-6
- Interface Restrictions, page 1-8

Command and Control Interface

The command and control interface has an IP address and is used for configuring the sensor. It receives security and status events from the sensor and queries the sensor for statistics.

The command and control interface is permanently enabled. It is permanently mapped to a specific physical interface, which depends on the specific model of sensor. You cannot use the command and control interface as either a sensing or alternate TCP reset interface.

Table 1-1 lists the command and control interfaces for each sensor.

Table 1-1 Command and Control Interfaces

Sensor	Command and Control Interface
IDS-4210	FastEthernet0/1
IDS-4215	FastEthernet0/0
IDS-4235	GigabitEthernet0/1
IDS-4250	GigabitEthernet0/1
IPS-4240	Management0/0
IPS-4255	Management0/0
IPS-4260	Management0/0
NM-CIDS	FastEthernet0/0
AIP-SSM-10	GigabitEthernet0/0
AIP-SSM-20	GigabitEthernet0/0
IDSM-2	GigabitEthernet0/2

Sensing Interfaces

Sensing interfaces are used by the sensor to analyze traffic for security violations. A sensor has one or more sensing interfaces depending on the sensor. For the number and type of sensing interfaces available for each sensor, see Interface Support, page 1-5.

Sensing interfaces can operate individually in promiscuous mode or you can pair them to create inline interfaces for inline sensing mode. For more information, see Promiscuous Mode, page 1-9, Inline Interface Mode, page 1-10, and Inline VLAN Pair Mode, page 1-10.

Note On appliances, all sensing interfaces are disabled by default. You must enable them to use them. On modules, the sensing interfaces are permanently enabled.

Some appliances support optional PCI interface cards that add sensing interfaces to the sensor. You must insert or remove these optional cards while the sensor is powered off. The sensor detects the addition or removal of a supported interface card. If you remove an optional PCI card, some of the interface configuration is deleted, such as the speed, duplex, description string, enabled/disabled state of the interface, and any inline interface pairings. These settings are restored to their default settings when the card is reinstalled. However, the assignment of promiscuous and inline interfaces to the Analysis Engine is not deleted from the Analysis Engine configuration, but is ignored until those cards are reinserted and you create the inline interface pairs again. For more information, refer to “Analysis Engine,” in *Installing*

and Using Cisco Intrusion Prevention System Device Manager Version 5.1 or "Assigning Interfaces to the Virtual Sensor," in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*.

Interface Support

Table 1-2 describes the interface support for appliances and modules running IPS 5.1:

Table 1-2 Interface Support

Base Chassis	Added PCI Cards	Interfaces Supporting Inline	Possible Port Combinations	Interfaces Not Supporting Inline
IDS-4210	—	None	N/A	All
IDS-4215	—	None	N/A	All
IDS-4215	4FE	FastEthernet0/1 4FE FastEthernetS/0[1] FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3 0/1<->1/0 0/1<->1/1 0/1<->1/2 0/1<->1/3	FastEthernet0/0
IDS-4235	—	None	N/A	All
IDS-4235	4FE	4FE FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4235	TX (GE)	TX onboard + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 or GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	—	None	N/A	All
IDS-4250	4FE	4FE FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4250	TX (GE)	TX onboard + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 or GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	SX	None	N/A	All

Table 1-2 Interface Support (continued)

Base Chassis	Added PCI Cards	Interfaces Supporting Inline	Possible Port Combinations	Interfaces Not Supporting Inline
IDS-4250	SX + SX	2 SX GigabitEthernet1/0 GigabitEthernet2/0	1/0<->2/0	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4250	XL	2 SX of the XL GigabitEthernet2/0 GigabitEthernet2/1	2/0<->2/1	GigabitEthernet0/0 GigabitEthernet0/1
IDSM-2	—	port 7 and 8 GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2
IPS-4240	—	4 onboard GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS-4255	—	4 onboard GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS-4260	—	4 onboard GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
NM-CIDS	—	None	N/A	All
AIP-SSM 10	—	GigabitEthernet0/1	By security context	GigabitEthernet0/0
AIP-SSM 20	—	GigabitEthernet0/1	By security context	GigabitEthernet0/0

1. The 4FE card can be installed in either slot 1 or 2. S indicates the slot number, which can be either 1 or 2.

TCP Reset Interfaces

Note The alternate TCP reset interface setting is ignored in inline interface or inline VLAN pair mode, because resets are sent inline in these modes.

This section explains the TCP reset interfaces and when to use them. It contains the following topics:

- Understanding Alternate TCP Reset Interfaces, page 1-7
- Designating the Alternate TCP Reset Interface, page 1-8

Understanding Alternate TCP Reset Interfaces

You can configure sensors to send TCP reset packets to try to reset a network connection between an attacker host and its intended target host. In some installations when the interface is operating in promiscuous mode, the sensor may not be able to send the TCP reset packets over the same sensing interface on which the attack was detected. In such cases, you can associate the sensing interface with an alternate TCP reset interface and any TCP resets that would otherwise be sent on the sensing interface when it is operating in promiscuous mode, are instead sent out on the associated alternate TCP reset interface. For more information, see Designating the Alternate TCP Reset Interface, page 1-8.

If a sensing interface is associated with an alternate TCP reset interface, that association applies when the sensor is configured for promiscuous mode but is ignored when the sensing interface is configured for inline mode.

With the exception of IDSM-2, any sensing interface can serve as the alternate TCP reset interface for another sensing interface. The alternate TCP reset interface on IDSM-2 is fixed because of hardware limitations.

Table 1-3 lists the alternate TCP reset interfaces.

Table 1-3 Alternate TCP Reset Interfaces

Sensor	Alternate TCP Reset Interface
IDS-4210	None[1]
IDS-4215	Any sensing interface
IDS-4235	Any sensing interface
IDS-4250	Any sensing interface
IPS-4240	Any sensing interface
IPS-4255	Any sensing interface
IPS-4260	Any sensing interface
NM-CIDS	None[2]
AIP-SSM-10	None[3]
AIP-SSM-20	None[4]
IDSM-2	System0/1[5]

1. There is only one sensing interface on IDS-4210.
2. There is only one sensing interface on NM-CIDS.
3. There is only one sensing interface on AIP-SSM-10.
4. There is only one sensing interface on AIP-SSM- 20.
5. This is an internal interface on the Catalyst backplane.

Designating the Alternate TCP Reset Interface

You need to designate an alternate TCP reset interface in the following situations:

- When a switch is being monitored with either SPAN or VACL capture and the switch does not accept incoming packets on the SPAN or VACL capture port.
- When a switch is being monitored with either SPAN or VACL capture for multiple VLANs, and the switch does not accept incoming packets with 802.1q headers.

Note The TCP resets need 802.1q headers to tell which VLAN the resets should be sent on.

- When a network tap is used for monitoring a connection.

Note Taps do not permit incoming traffic from the sensor.

You can only assign a sensing interface as an alternate TCP reset interface. You cannot configure the management interface as an alternate TCP reset interface

Interface Restrictions

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
  - On modules (IDSM-2, NM-CIDS, AIP-SSM-10, and AIP-SSM-20) and IPS-4240, IPS-4255, and IPS-4260 all backplane interfaces have fixed speed, duplex, and state settings. These settings are protected in the default configuration on all backplane interfaces.
  - For nonbackplane FastEthernet interfaces the valid speed settings are 10 Mbps, 100 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit fiber interfaces (1000-SX and XL on the IDS-4250), valid speed settings are 1000 Mbps and auto.
  - For Gigabit copper interfaces (1000-TX on the IDS-4235, IDS-4250, IPS-4240, IPS-4255, and IPS-4260), valid speed settings are 10 Mbps, 100 Mbps, 1000 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit (copper or fiber) interfaces, if the speed is configured for 1000 Mbps, the only valid duplex setting is auto.
  - The command and control interface cannot also serve as a sensing interface.
- Inline Interface Pairs
  - Inline interface pairs can contain any combination of sensing interfaces regardless of the physical interface type (copper versus fiber), speed, or duplex settings of the interface. However, pairing interfaces of different media type, speeds, and duplex settings may not be fully tested or officially supported. For more information, see Interface Support, page 1-5.
  - The command and control interface cannot be a member of an inline interface pair.
  - You cannot pair a physical interface with itself in an inline interface pair.
  - A physical interface can be a member of only one inline interface pair.

  - You can only configure bypass mode and create inline interface pairs on sensor platforms that support inline mode.
  - A physical interface cannot be a member of an inline interface pair unless the subinterface mode of the physical interface is **none**.
- Inline VLAN Pairs
  - You cannot pair a VLAN with itself.
  - For a given sensing interface, a VLAN can be a member of only one inline VLAN pair. However, a given VLAN can be a member of an inline VLAN pair on more than one sensing interface.
  - The order in which you specify the VLANs in an inline VLAN pair is not significant.
  - A sensing interface in inline VLAN pair mode can have from 1 to 255 inline VLAN pairs.
- Alternate TCP Reset Interface:
  - You can only assign the alternate TCP reset interface to a sensing interface. You cannot configure the command and control interface as an alternate TCP reset interface. The alternate TCP reset interface option is set to **none** as the default and is protected for all interfaces except the sensing interfaces.
  - You can assign the same physical interface as an alternate TCP reset interface for multiple sensing interfaces.
  - A physical interface can serve as both a sensing interface and an alternate TCP reset interface.
  - The command and control interface cannot serve as the alternate TCP reset interface for a sensing interface.
  - A sensing interface cannot serve as its own alternate TCP reset interface.
  - You can only configure interfaces that are capable of TCP resets as alternate TCP reset interfaces.

Note The exception to this restriction is the IDSM-2. The alternate TCP reset interface assignments for both sensing interfaces is System0/1 (protected).

Interface Modes

The following section describes the interface modes and contains the following topics:

- Promiscuous Mode, page 1-9
- Inline Interface Mode, page 1-10
- Inline VLAN Pair Mode, page 1-10

Promiscuous Mode

In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response

actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).

Inline Interface Mode

Operating in inline interface mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (layers 3 to 7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.

In inline interface mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

Note You can configure AIP-SSM to operate inline even though it has only one sensing interface.

Note If the paired interfaces are connected to the same switch, you should configure them on the switch as access ports with different access VLANs for the two ports. Otherwise, traffic does not flow through the inline interface.

Inline VLAN Pair Mode

You can associate VLANs in pairs on a physical interface. This is known as inline VLAN pair mode. Packets received on one of the paired VLANs are analyzed and then forwarded to the other VLAN in the pair. Inline VLAN pairs are supported on all sensors that are compatible with IPS 5.1 except NM-CIDS, AIP-SSM-10, and AIP-SSM-20.

Inline VLAN pair mode is an active sensing mode where a sensing interface acts as an 802.1q trunk port, and the sensor performs VLAN bridging between pairs of VLANs on the trunk. The sensor inspects the traffic it receives on each VLAN in each pair, and can either forward the packets on the other VLAN in the pair, or drop the packet if an intrusion attempt is detected. You can configure an IPS sensor to simultaneously bridge up to 255 VLAN pairs on each sensing interface. The sensor replaces the VLAN ID field in the 802.1q header of each received packet with the ID of the egress VLAN on which the sensor forwards the packet. The sensor drops all packets received on any VLANs that are not assigned to inline VLAN pairs.

Your Network Topology

Before you deploy and configure your sensors, you should understand the following about your network:

- The size and complexity of your network.
- Connections between your network and other networks (and the Internet).
- The amount and type of network traffic on your network.

This knowledge will help you determine how many sensors are required, the hardware configuration for each sensor (for example, the size and type of network interface cards), and how many managers are needed.

Supported Sensors

Table 1-4 lists the sensors (appliances and modules) that are supported by Cisco IPS 5.1.

Note For instructions on how to obtain the most recent Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

Caution Installing the most recent software (version 5.1) on unsupported sensors may yield unpredictable results. We do not support software installed on unsupported platforms.

Table 1-4 Supported Sensors

Model Name	Part Number	Optional Interfaces
Appliances		
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	— — —
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9[1]	IDS-4FE-INT= —
IDS-4235	IDS-4235-K9 IDS-4235-TX-K9	IDS-4FE-INT= IDS-TX-INT=
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	IDS-4FE-INT= IDS-4250-SX-INT=[2] IDS-XL-INT= IDS-TX-INT= — —

Table 1-4 Supported Sensors (continued)

Model Name	Part Number	Optional Interfaces
Appliances		
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9[3]	— —
IPS-4255	IPS-4255-K9	—
IPS-4260	IPS-4260-K9 IPS-4260-4GE-BP-K9 IPS-4260-2SX-K9	IPS-4GE-BP-INT= IPS-2SX-INT= — —
Modules		
AIP-SSM-10	ASA-SSM-AIP-10-K9	—
AIP-SSM-20	ASA-SSM-AIP-20-K9	—
IDSM-2	WS-SVC-IDSM2-K9	—
NM-CIDS	NM-CIDS-K9	—

1. IDS-4215-4FE-K9 is the IDS-4215-K9 with the optional 4FE card (IDS-4FE-INT=) installed at the factory.
2. You can install one or two IDS-4250-SX-INT cards in the IDS-4250.
3. IPS-4240-DC-K9 is a NEBS-compliant product.

The following NRS and IDS appliance models are legacy models and are not supported in this document:

- NRS-2E
- NRS-2E-DM
- NRS-2FE
- NRS-2FE-DM
- NRS-TR
- NRS-TR-DM
- NRS-SFDDI
- NRS-SFDDI-DM
- NRS-DFDDI
- NRS-DFDDI-DM
- IDS-4220-E
- IDS-4220-TR
- IDS-4230-FE
- IDS-4230-SFDDI
- IDS-4230-DFDDI

Note The WS-X6381, the IDSM, is a legacy model and is not supported in this document.

Note IDS-4210 requires a memory upgrade to support the most recent IPS software. For more information, see Upgrading the Memory, page 2-3.

Appliances

This section describes the Cisco 4200 series appliance and contains the following topics:

- Introducing the Appliance, page 1-13
- Appliance Restrictions, page 1-14
- Setting Up a Terminal Server, page 1-14

Introducing the Appliance

The appliance is a high-performance, plug-and-play device. The appliance is a component of the IPS, a network-based, real-time intrusion prevention system. For a list of supported appliances, see Supported Sensors, page 1-11.

You can use the CLI, IDM, or ASDM to configure the appliance. Refer to the *Documentation Roadmap for Cisco Intrusion Prevention System 5.1* that shipped with your appliance for the list of IPS documents and how to access them.

You can configure the appliance to respond to recognized signatures as it captures and analyzes network traffic. These responses include logging the event, forwarding the event to the manager, performing a TCP reset, generating an IP log, capturing the alert trigger packet, and reconfiguring a router. The appliance offer significant protection to your network by helping to detect, classify, and stop threats including worms, spyware and adware, network viruses, and application abuse.

After being installed at key points in the network, the appliance monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, appliances can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the manager. Other legitimate connections continue to operate independently without interruption.

Appliances are optimized for specific data rates and are packaged in Ethernet, Fast Ethernet, and Gigabit Ethernet configurations. In switched environments, appliances must be connected to the switch SPAN port or VACL capture port.

The Cisco IPS 4200 series appliances provide the following:

- Protection of multiple network subnets through the use of up to eight interfaces
- Simultaneous, dual operation in both promiscuous and inline modes
- A wide array of performance options—from 80 Mbps to multiple gigabits
- Embedded web-based management solutions packaged with the sensor

Appliance Restrictions

The following restrictions apply to using and operating the appliance:

- The appliance is not a general purpose workstation.
- Cisco Systems prohibits using the appliance for anything other than operating Cisco IPS.
- Cisco Systems prohibits modifying or installing any hardware or software in the appliance that is not part of the normal operation of the Cisco IPS.

Setting Up a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For IDS-4215, IPS-4240, IPS-4255, and IPS-4260:
  - For RJ-45 connections, connect a 180 rollover cable from the console port on the appliance to a port on the terminal server.
  - For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.
- For all other appliances, connect the M.A.S.H. adapter (part number 29-4077-01) to COM1 on the appliance and:
  - For RJ-45 connections, connect a 180 rollover cable from the M.A.S.H. adapter to a port on the terminal server.
  - For hydra cable assemblies, connect a straight-through patch cable from the M.A.S.H. adapter to a port on the terminal server.

Step 2 Configure the line and port on the terminal server as follows:

a. In enable mode, type the following configuration, where # is the line number of the port to be configured:

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

b. If you are configuring a terminal server for an IDS-4215, IPS-4240, IPS-4255, or IPS-4260 go to Step 3.

Otherwise, for all other supported appliances, to direct all output to the terminal server, log in to the CLI and type the following commands:

```
sensor# configure terminal
sensor(config)# display-serial
```

Output is directed to the serial port. Use the **no display-serial** command to redirect output to the keyboard and monitor.

Note You can set up a terminal server and use the **display-serial** command to direct all output from the appliance to the serial port. This option lets you view system messages on a console connected to the serial port, even during the boot process. When you use this option, all output is directed to the serial port and any local keyboard and monitor connection is disabled. However, BIOS and POST messages are still displayed on the local keyboard and monitor. For the procedure, see "Displaying Output to a Serial Connection," in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*.

Note There are no keyboard or monitor ports on an IDS-4215, IPS-4240, IPS-4255, or IPS-4260; therefore, the **display-serial** and **no display-serial** commands do not apply to those platforms.

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance.

If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

Modules

This section describes the modules and contains the following topics:

- Introducing AIP-SSM, page 1-15
- Introducing IDSM-2, page 1-16
- Introducing NM-CIDS, page 1-17

Introducing AIP-SSM

The Cisco ASA Advanced Inspection and Prevention Security Services Module (SSM) is the IPS plug-in module in the Cisco ASA 5500 series adaptive security appliance (ASA). The ASA software combines firewall, VPN concentrator, and intrusion detection and prevention software functionality into one software image.

There are two models of AIP-SSM: ASA-SSM-AIP-K9-10 and ASA-SSM-AIP-K9-20. ASA-SSM-AIP-K9-10 supports approximately 100 Mbps throughput and ASA-SSM-AIP-K9-20 supports approximately 200 Mbps. Only one module can populate the slot in an ASA at a time.

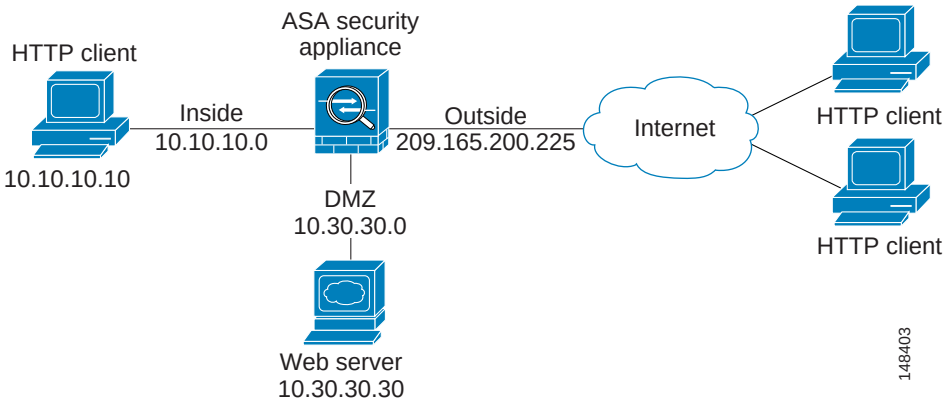
AIP-SSM runs advanced IPS software that provides further security inspection in either inline mode or promiscuous mode. The ASA diverts packets to AIP-SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to AIP-SSM.

In promiscuous mode, the IPS receives packets over the GigabitEthernet interface, examines them for intrusive behavior, and generates alerts based on a positive result of the examination. In inline mode, there is the additional step of sending all packets, which did not result in an intrusion, back out the GigabitEthernet interface.

Figure 1-2 shows ASA with AIP-SSM in a typical DMZ configuration. A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network. The web server is on the DMZ interface, and HTTP clients from both the inside and outside networks can access the web server securely.

In Figure 1-2 an HTTP client (10.10.10.10) on the inside network initiates HTTP communications with the DMZ web server (30.30.30.30). HTTP access to the DMZ web server is provided for all clients on the Internet; all other communications are denied. The network is configured to use an IP pool (a range of IP addresses available to the DMZ interface) of addresses between 30.30.30.50 and 30.30.30.60.

Figure 1-2 DMZ Configuration



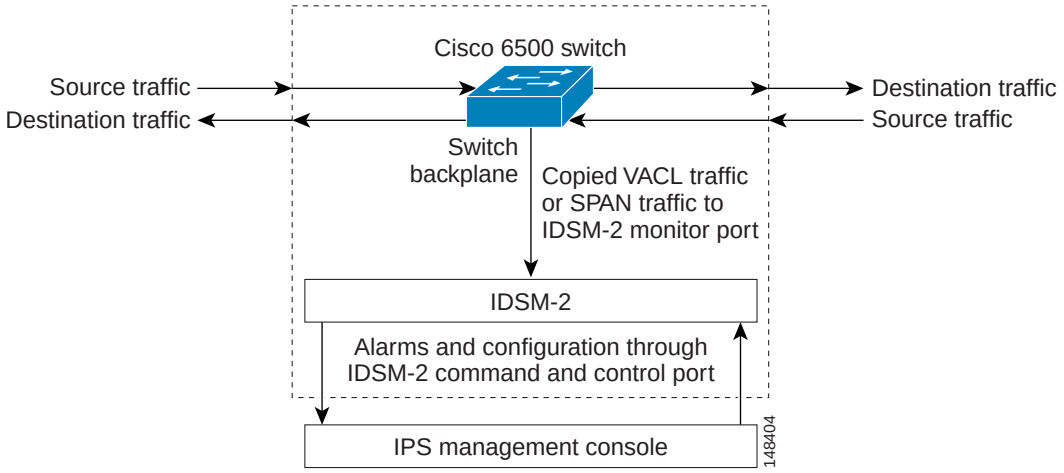
Refer to *Cisco ASA 5500 Quick Start Guide*for more information on setting up ASA. For more information on installing AIP-SSM, see Installing AIP-SSM, page 7-3. For more information on configuring AIP-SSM to receive IPS traffic, refer to "Configuring AIP-SSM," in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*.

Introducing IDSM-2

The Cisco Catalyst 6500 Series Intrusion Detection System Services Module (IDSM-2) is a switching module that performs intrusion prevention in the Catalyst 6500 series switch and 7600 series router. You can use the CLI or IDSM to configure IDSM-2. You can configure IDSM-2 for promiscuous or inline mode.

IDSM-2 performs network sensing—real-time monitoring of network packets through packet capture and analysis. IDSM-2 captures network packets and then reassembles and compares the packet data against attack signatures indicating typical intrusion activity. Network traffic is either copied to IDSM-2 based on security VACLs in the switch or is copied to IDSM-2 through the switch's SPAN port feature. These methods route user-specified traffic to IDSM-2 based on switch ports, VLANs, or traffic type to be inspected. (See Figure 1-3.)

Figure 1-3 IDSM-2 Block Diagram



IDSM-2 searches for patterns of misuse by examining either the data portion and/or the header portion of network packets. Content-based attacks contain potentially malicious data in the packet payload, whereas, context-based attacks contain potentially malicious data in the packet headers.

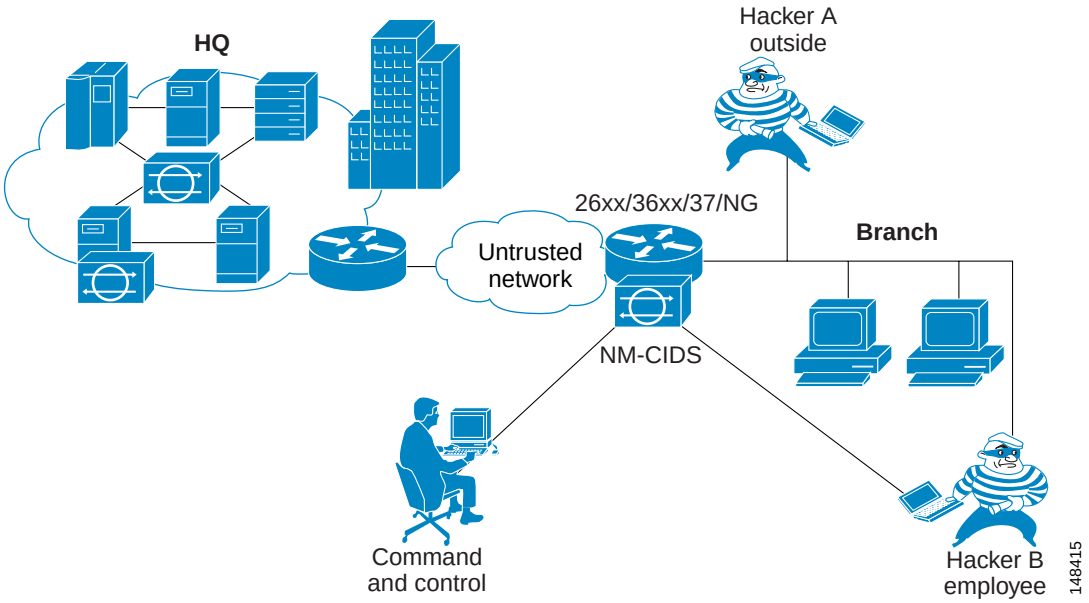
You can configure IDSM-2 to generate an alert when it detects potential attacks. Additionally, you can configure IDSM-2 to transmit TCP resets on the source VLAN, generate an IP log, and/or initiate blocking countermeasures on a firewall or other managed device. Alerts are generated by IDSM-2 through the Catalyst 6500 series switch backplane to the IPS manager, where they are logged or displayed on a graphical user interface.

Introducing NM-CIDS

The Cisco Intrusion Detection System Network Module (NM-CIDS) integrates the Cisco IDS functionality into a branch office router. With NM-CIDS, you can implement full-featured IDS at your remote branch offices. You can install NM-CIDS in any one of the network module slots on the Cisco 2600, 3600, and 3700 series routers. NM-CIDS can monitor up to 45 Mbps of network traffic. For a list of supported routers, see Software and Hardware Requirements, page 9-2. Only one NM-CIDS is supported per router. Figure 1-4 on page 1-18 shows the router in a branch office environment.

Note NM-CIDS operates in promiscuous mode (IDS mode) only.

Figure 1-4 NM-CIDS in the Branch Office Router



NM-CIDS has one internal 10/100 Ethernet port that connects to the router's backplane. There is also one external 10/100-based Ethernet port that is used for device management (management of other routers and/or PIX Firewalls to perform blocking) and command and control of NM-CIDS by IDS managers.

NM-CIDS communicates with the router to exchange control and state information for bringing up and shutting down NM-CIDS and to exchange version and status information. NM-CIDS processes packets that are forwarded from selected interfaces on the router to the IDS interface on NM-CIDS. NM-CIDS analyzes the captured packets and compares them against a rule set of typical intrusion activity called signatures. If the captured packets match a defined intrusion pattern in the signatures, NM-CIDS can take one of two actions: it can make ACL changes on the router to block the attack, or it can send a TCP reset packet to the sender to stop the TCP session that is causing the attack.

In addition to analyzing captured packets to identify malicious activity, NM-CIDS can also perform IP session logging that can be configured as a response action on a per-signature basis. When the signature fires, session logs are created over a specified time period in a tcpdump format. You can view these logs using Ethereal or replay the IP session using tools such as TCP Replay.

You can manage and retrieve events from NM-CIDS through the CLI or IDM.

The IDS requires a reliable time source. All the events (alerts) must have the correct time stamp, otherwise, you cannot correctly analyze the logs after an attack. You cannot manually set the time on NM-CIDS. NM-CIDS gets its time from the Cisco router in which it is installed. Routers do not have a battery so they cannot preserve a time setting when they are powered off. You must set the router's clock each time you power up or reset the router, or you can configure the router to use NTP time synchronization. We recommend NTP time synchronization. You can configure either NM-CIDS itself or the router it is installed in to use NTP time synchronization. For more information, see Time Sources and the Sensor, page 1-19.

Time Sources and the Sensor

This section explains the importance of having a reliable time source for the sensors and how to correct the time if there is an error.

This section contains the following topics:

- Understanding Time on the Sensor, page 1-19
- Correcting the Time on the Sensor, page 1-21

Understanding Time on the Sensor

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings. For more information, see Initializing the Sensor, page 10-2.

Here is a summary of ways to set the time on sensors:

- For appliances
  - Use the **clock set** command to set the time. This is the default.

    For the procedure, refer to "Manually Setting the Clock," *in Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*.
  - Use NTP

    You can configure the appliance to get its time from an NTP time synchronization source. Refer to "Configuring a Cisco Router to be an NTP Server," in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can set up NTP on the appliance during initialization or you can configure NTP through the CLI, IDM, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

- For IDSM-2
  - The IDSM-2 can automatically synchronize its clock with the switch time. This is the default.

    Note The UTC time is synchronized between the switch and the IDSM-2. The time zone and summertime settings are not synchronized between the switch and the IDSM-2.

Caution Be sure to set the time zone and summertime settings on both the switch and IDSM-2 to ensure that the UTC time settings are correct. IDSM-2's local time could be incorrect if the time zone and/or summertime settings do not match between IDSM-2 and the switch.

– Use NTP

You can configure IDSM-2 to get its time from an NTP time synchronization source. Refer to "Configuring a Cisco Router to be an NTP Server," in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure IDSM-2 to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

Note We recommend that you use an NTP time synchronization source.

- For NM-CIDS
  - NM-CIDS can automatically synchronize its clock with the clock in the router chassis in which it is installed (parent router). This is the default.

Note The UTC time is synchronized between the parent router and NM-CIDS. The time zone and summertime settings are not synchronized between the parent router and NM-CIDS.

Caution Be sure to set the time zone and summertime settings on both the parent router and NM-CIDS to ensure that the UTC time settings are correct. NM-CIDS's local time could be incorrect if the time zone and/or summertime settings do not match between NM-CIDS and the router.

– Use NTP

You can configure NM-CIDS to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. Refer to "Configuring a Cisco Router to be an NTP Server," in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure NM-CIDS to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

Note We recommend that you use an NTP time synchronization source.

- For AIP-SSM:
  - AIP-SSM can automatically synchronize its clock with the clock in the ASA in which it is installed. This is the default.

Note The UTC time is synchronized between ASA and AIP-SSM. The time zone and summertime settings are not synchronized between ASA and AIP-SSM.

Caution Be sure to set the time zone and summertime settings on both ASA and AIP-SSM to ensure that the UTC time settings are correct. The local time of AIP-SSM could be incorrect if the time zone and/or summertime settings do not match between AIP-SSM and ASA.

– Use NTP

You can configure AIP-SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. Refer to "Configuring a Cisco Router to be an NTP Server," in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure AIP-SSM to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

Note We recommend that you use an NTP time synchronization source.

Correcting the Time on the Sensor

If you set the time incorrectly, your stored events will have the incorrect time because they are stamped with the time the event was created.

The Event Store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command. For more information on the **clear events** command, refer to "Clearing Events from the Event Store," in *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*.

Caution You cannot remove individual events.

Installation Preparation

To prepare for installing sensors, follow these steps:

Step 1 Review the safety precautions outlined in the *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor* that shipped with your sensor.

Step 2 To familiarize yourself with the IPS and related documentation and where to find it on Cisco.com, read the *Documentation Roadmap for Cisco Intrusion Prevention System 5.1* that shipped with your sensor.

Step 3 Obtain the *Release Notes for Cisco Intrusion Prevention System 5.1* from Cisco.com and completely read them before proceeding with the installation.

Step 4 Unpack the sensor.

Step 5 Place the sensor in an ESD-controlled environment.

For more information, see Site and Safety Guidelines, page 1-22.

Step 6 Place the sensor on a stable work surface.

Step 7 Refer to the chapter that pertains to your sensor model.

Site and Safety Guidelines

This section describes site guidelines and safety precautions to take when working with electricity, with power supplies, and in an ESD environment. It contains the following topics:

- Site Guidelines, page 1-22
- Rack Configuration Guidelines, page 1-23
- Electrical Safety Guidelines, page 1-23
- Power Supply Guidelines, page 1-24
- Working in an ESD Environment, page 1-24

Site Guidelines

Place the appliance on a desktop or mount it in a rack. The location of the appliance and the layout of the equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause system malfunctions and shutdowns, and can make appliance maintenance difficult.

When planning the site layout and equipment locations, keep in mind the following precautions to help avoid equipment failures and reduce the possibility of environmentally-caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions may help you isolate the cause of failures and prevent future problems.

- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Make sure that the room in which you operate your system has adequate air circulation.
- Always follow the ESD-prevention procedures to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Make sure that the chassis top panel is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which can interrupt and redirect the flow of cooling air from the internal components.

Rack Configuration Guidelines

Follow these guidelines to plan your equipment rack configuration:

- Enclosed racks must have adequate ventilation. Make sure the rack is not overly congested because each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, make sure the rack frame does not block the intake or exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Make sure you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack. Experiment with different arrangements to position the baffles effectively.

Electrical Safety Guidelines

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.**

Follow these guidelines when working on equipment powered by electricity:

- Before beginning procedures that require access to the interior of the chassis, locate the emergency power-off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected from a circuit; always check the circuit.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs, proceed as follows:
  - Use caution; do not become a victim yourself.
  - Disconnect power from the system.
  - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim and then call for help.
  - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the chassis within its marked electrical ratings and product usage instructions.
- Install the sensor in compliance with local and national electrical codes as listed in the *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor* document.

- The sensor models equipped with AC-input power supplies are shipped with a 3-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. This is a safety feature that you should not circumvent. Equipment grounding should comply with local and national electrical codes.
- The sensor models equipped with DC-input power supplies must be terminated with the DC input wiring on a DC source capable of supplying at least 15 amps. A 15-amp circuit breaker is required at the 48 VDC facility power source. An easily accessible disconnect device should be incorporated into the facility wiring. Be sure to connect the grounding wire conduit to a solid earth ground. We recommend that you use a Listed closed-loop ring to terminate the ground conductor at the ground stud. The DC return connection to this system is to remain isolated from the system frame and chassis.

  Other DC power guidelines are listed in the *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor* document.

Power Supply Guidelines

Follow these guidelines for power supplies:

- Check the power at the site before installing the chassis to ensure that the power is free of spikes and noise. Install a power conditioner if necessary, to ensure proper voltages and power levels in the source voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The following applies to a chassis equipped with an AC-input power supply:
  - The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct AC-input power requirement.
  - Several types of AC-input power supply cords are available; make sure you have the correct type for your site.
  - Install a UPS for your site.
  - Install proper site-grounding facilities to guard against damage from lightning or power surges.
- The following applies to a chassis equipped with a DC-input power supply:
  - Each DC-input power supply requires dedicated 15-amp service.
  - For DC power cables, we recommend a minimum of 14 AWG wire cable.
  - The DC return connection to this system is to remain isolated from the system frame and chassis.

Working in an ESD Environment

Work on ESD-sensitive parts only at an approved static-safe station on a grounded static dissipative work surface, for example, an ESD workbench or static dissipative mat.

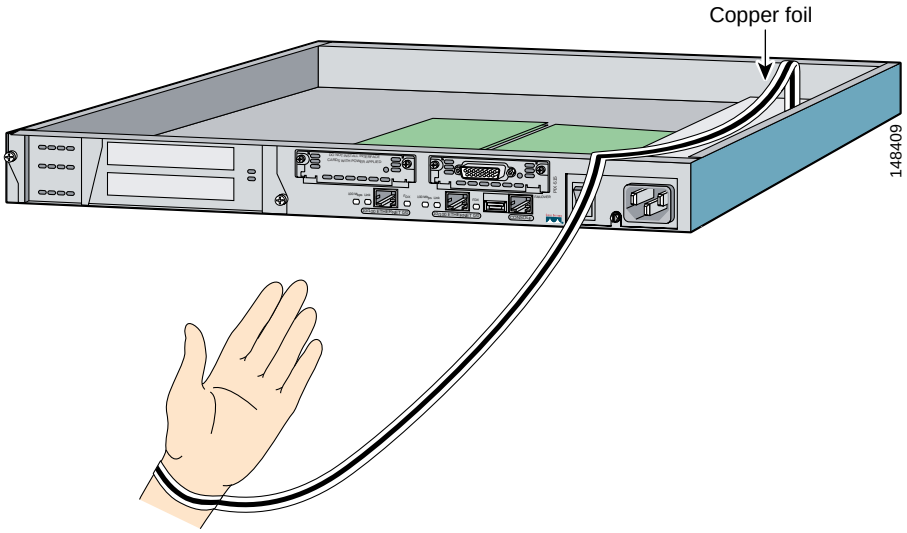
To remove and replace components in a sensor, follow these steps:

Step 1 Remove all static-generating items from your work area.

Step 2 Use a static dissipative work surface and wrist strap.

Note Disposable wrist straps, typically those included with an upgrade part, are designed for one time use.

Step 3 Attach the wrist strap to your wrist and to the terminal on the work surface. If you are using a disposable wrist strap, connect the wrist strap directly to an unpainted metal surface of the chassis.



Step 4 Connect the work surface to the chassis using a grounding cable and alligator clip.

Caution Always follow ESD-prevention procedures when removing, replacing, or repairing components.

Note If you are upgrading a component, do not remove the component from the ESD packaging until you are ready to install it.

Cable Pinouts

This section describes pinout information for 10/100/1000BaseT, console, and RJ 45 to DB 9 ports, and the MGMT 10/100 Ethernet port. This section contains the following topics:

- 10/100BaseT and 10/100/1000BaseT Connectors, page 1-25
- Console Port (RJ-45), page 1-26
- RJ-45 to DB-9 or DB-25, page 1-27

10/100BaseT and 10/100/1000BaseT Connectors

Sensors support 10/100/1000BaseT ports. You must use at least a Category 5 cable for 100/1000Base-TX operations. You can use a Category 3 cable for 10Base-TX operations.

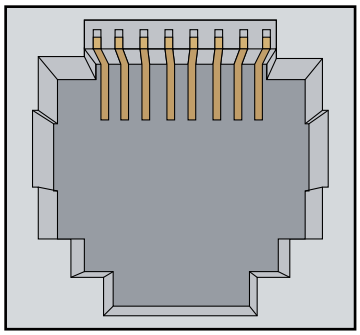
Note Some sensors support 10/100BaseT (IDS-4210, IDS-4215, and the optional 4FE card) while others support 10/100/1000BaseT (IDS-4235, IDS-4250-TX, IPS-4240, IPS-4255, and IPS-4260). This only applies to the copper appliances. The fiber appliances support 1000Base-SX only.

The 10/100/1000BaseT ports use standard RJ-45 connectors and support MDI and MDI-X connectors. Ethernet ports normally use MDI connectors and Ethernet ports on a hub normally use MDI-X connectors.

An Ethernet straight-through cable is used to connect an MDI to an MDI-X port. A cross-over cable is used to connect an MDI to an MDI port, or an MDI-X to an MDI-X port.

Figure 1-5 shows the 10/100BaseT (RJ-45) port pinouts.

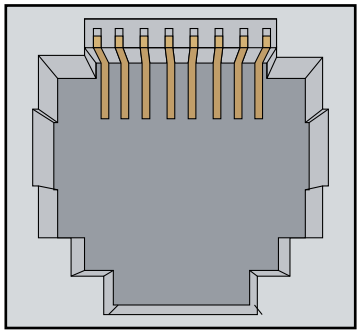
Figure 1-5 10/100 Port Pinouts

Pin	Label	1 2 3 4 5 6 7 8
1	TD+	
2	TD-	
3	RD+	
4	NC	
5	NC	
6	RD-	
7	NC	
8	NC	

148407

Figure 1-6 shows the 10/100/1000BaseT (RJ-45) port pinouts.

Figure 1-6 10/100/1000 Port Pinouts

Pin	Label	1 2 3 4 5 6 7 8
1	TP0+	
2	TP0-	
3	TP1+	
4	TP2+	
5	TP2-	
6	TP1-	
7	TP3+	
8	TP3-	

148410

Console Port (RJ-45)

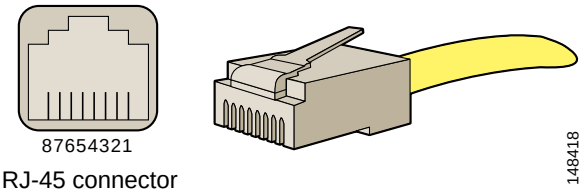
Cisco products use the following types of RJ-45 cables:

- Straight-through
- Cross-over
- Rolled (console)

Note Cisco does not provide these cables; however, they are widely available from other sources.

Figure 1-7 shows the RJ 45 cable.

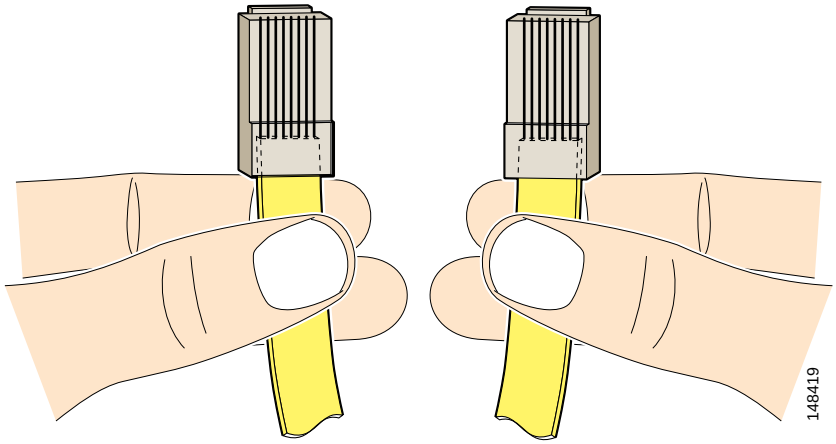
Figure 1-7 RJ-45 Cable



RJ-45 connector

To identify the RJ-45 cable type, hold the two ends of the cable next to each other so that you can see the colored wires inside the ends, as shown in Figure 1-8.

Figure 1-8 RJ-45 Cable Identification



Examine the sequence of colored wires to determine the type of RJ-45 cable, as follows:

- Straight-through—The colored wires are in the same sequence at both ends of the cable.
- Cross-over—The first (far left) colored wire at one end of the cable is the third colored wire at the other end of the cable.
- Rolled—The colored wires are in the opposite sequence at either end of the cable.

RJ-45 to DB-9 or DB-25

Table 1-5 lists the cable pinouts for RJ-45 to DB-9 or DB-25.

Table 1-5 Cable Pinouts for RJ-45 to DB-9 or DB-25

Signal	RJ-45 Pin	DB-9 /DB-25 Pin
RTS	8	8
DTR	7	6
TxD	6	2
GND	5	5
GND	4	5
RxD	3	3
DSR	2	4
CTS	1	7